IN THE CLAIMS

Amended claims follow:

1. (currently amended): A system for providing a framework for network appliance management in a distributed computing environment, comprising:

an appliance status table recording a status report periodically received from a status daemon autonomously operating on each of a plurality of network appliances, each status report containing health and status information and application-specific data pertaining to autonomous configuration and management of each network appliance; and

a catalog server maintaining configuration settings for each network appliance progressively assembled concurrent to providing installable components and dynamically providing a catalog listing currently installable components for being installed on each network appliance based on the configuration settings independently received from the network appliance;

wherein each network appliance, prior to sending the status report, executes at least one initial plug-in; and, after installing the installable components, executes at least one post-plug-in;

wherein the at least one initial plug-in monitors the status daemon to determine if the status daemon is running, and restart the status daemon if it is determined that the status daemon is not running;

wherein the catalog further includes installable component names, installable component versions, a tag indicating a component server at which to locate and obtain each installable component, and a type indicator indicating whether each installable component is a package or a file;

wherein a network operations center establishes a secure session with each network appliance utilizing Secure Hypertext Transfer Protocol (HTTPS);

wherein the appliance status table further records a user identifier associated with one of the network appliances from which the status report is received and a time the status report is received.

2. (cancelled)

3. (currently amended): A system according to Claim 1, [further comprising:

a] wherein the network operations center install[ing]s an initial set of installable components on each network appliance during a bootstrap configuration.

4. (previously presented): A system according to Claim 1, wherein the currently installable components comprise at least one self-installable package, and the component server supplies the at least one package for installation responsive to a request from one such network appliance.

5. (original): A system according to Claim 4, further comprising:

a crypto module digitally signing the at least one package for the network operations center prior to being supplied for installation.

6. (original): A system according to Claim 4, further comprising:

a crypto module encrypting the at least one package prior to being supplied for installation.

7. (previously presented): A system according to Claim 1, wherein the installable components comprise at least one file, and the component server supplies the at least one file responsive to a request from one such network appliance.

8. (currently amended): A system according to Claim 7, wherein the component server establishes [a]the secure session prior to the at least one file being supplied for installation.

9. (original): A system according to Claim 7, further comprising:

a file information subdirectory specifying installation instructions for the at least one file in a pre-determined entry prior to the at least one file being supplied for installation.

10. (original): A system according to Claim 1, further comprising:

a proxy component server staging the currently installable components for retrieval in a separate components database.

11. (original): A system according to Claim 1, wherein the distributed computing environment is TCP/IP-compliant.

12. (currently amended): A method for providing a framework for network appliance management in a distributed computing environment, comprising:

recording a status report periodically received from a status daemon autonomously operating on each of a plurality of network appliances, each status report containing health and status information and application-specific data pertaining to autonomous configuration and management of each network appliance;

maintaining configuration settings for each network appliance progressively assembled concurrent to providing installable components; and

dynamically providing a catalog listing currently installable components for being installed on each network appliance based on the configuration settings independently received from the network appliance;

wherein each network appliance, prior to sending the status report, executes at least one initial plug-in; and, after installing the installable components, executes at least one post-plug-in;

wherein the at least one initial plug-in monitors the status daemon to determine if the status daemon is running, and restart the status daemon if it is determined that the status daemon is not running;

wherein the catalog further includes installable component names, installable component versions, a tag indicating a component server at which to locate and obtain each installable component, and a type indicator indicating whether each installable component is a package or a file;

wherein a secure session is established with each network appliance utilizing Secure Hypertext Transfer Protocol (HTTPS);

wherein a user identifier associated with one of the network appliances from which the status report is received and a time the status report is received are recorded.

13. (cancelled)

14. (original): A method according to Claim 12, further comprising:

installing an initial set of installable components on each network appliance during a bootstrap configuration.

15. (original): A method according to Claim 12, wherein the currently installable components comprise at least one self-installable package, further comprising:

supplying the at least one package for installation responsive to a request from one such network appliance.

16. (original): A method according to Claim 15, further comprising:

digitally signing the at least one package prior to being supplied for installation.

17. (original): A method according to Claim 15, further comprising:

encrypting the at least one package prior to being supplied for installation.

18. (original): A method according to Claim 12, wherein the installable components comprise at least one file, further comprising:

supplying the at least one file responsive to a request from one such network appliance.

19. (currently amended): A method according to Claim 18, further comprising:

establishing [a]the secure session prior to the at least one file being supplied for installation.

20. (original): A method according to Claim 18, further comprising:

specifying installation instructions for the at least one file in a pre-determined entry prior to the at least one file being supplied for installation.

21. (original): A method according to Claim 12, further comprising:

staging the currently installable components for retrieval in a separate components database.

22. (original): A method according to Claim 12, wherein the distributed computing environment is TCP/IP-compliant.

23. (currently amended): A computer-readable storage medium holding code for performing the method according to Claims 12,[13,] 14, 15, 16, 17, 18, 19, 20, 21, or 22.

24. (currently amended): A system for autonomously managing a network appliance deployed within a distributed computing environment, comprising:

an internal catalog of components installed on one such network appliance identified by component and version; and

a status daemon operating autonomously on the one such network appliance and periodically providing a status report containing health and status information and application-specific data pertaining to autonomous configuration and management of the one such network appliance; and

a catalog checker obtaining a catalog of currently installable components dynamically generated for the one such network appliance based on the status report independently received from the one such network appliance and determining non-current components by comparing the components and versions listed in the obtained catalog against the internal catalog;

wherein each network appliance, prior to sending the status report, executes at least one initial plug-in; and, after installing the installable components, executes at least one post-plug-in;

wherein the at least one initial plug-in monitors the status daemon to determine if the status daemon is running, and restart the status daemon if it is determined that the status daemon is not running;

wherein the catalog further includes a tag indicating a component server at which to locate and obtain each installable component, and a type indicator indicating whether each installable component is a package or a file;

wherein a network operations center negotiates a secure session with the one such network appliance utilizing Secure Hypertext Transfer Protocol (HTTPS);

wherein an appliance status table records a user identifier associated with the one such network appliance from which the status report is received and a time the status report is received.

25. (cancelled)

26. (cancelled)

27. (cancelled)

28. (cancelled)

29. (original): A system according to Claim 24, wherein the components comprise at least one self-installable package, further comprising:

an installer obtaining the at least one self-installable package and installing the at least one self-installable package per instructions encoded therein.

30. (original): A system according to Claim 29, wherein the components further comprise at least one file dependent on the at least one self-installable package, further comprising:

an installer obtaining the at least one file subsequent to installing the at least one self-installable package and installing the at least one self-installable package per instructions stored in a pre-determined entry.

31. (previously presented): A system according to Claim 29, wherein the component server negotiates a non-secure session prior to obtaining the at least one self-installable package.

32. (original): A system according to Claim 29, further comprising:

a crypto module at least one of authenticating and decrypting the at least one self-installable package prior to installing the at least one self-installable package.

33. (original): A system according to Claim 29, wherein the instructions comprise an executable installation program plus one or more files to be installed.

34. (original): A system according to Claim 29, wherein the components further comprise at least one file, further comprising:

an installer obtaining the at least one file and installing the at least one self-installable package per instructions stored in a pre-determined entry.

35. (currently amended): A system according to Claim 34, wherein the component server negotiates [a]the secure session prior to obtaining the at least one self-installable package.

36. (original): A system according to Claim 34, wherein the pre-determined entry comprise a file information subdirectory identifying installation instructions.

37. (original): A system according to Claim 29, wherein at least one such network appliance performs one of electronic mail anti-virus scanning, content filtering, packet routing, and file, Web and print servicing.

38. (original): A system according to Claim 29, wherein the distributed computing environment is TCP/IP-compliant.

39. (currently amended): A method for autonomously managing a network appliance deployed within a distributed computing environment, comprising:

maintaining an internal catalog of components installed on one such network appliance identified by component and version;

periodically providing a status report containing health and status information and application-specific data pertaining to autonomous configuration and management of the one such network appliance and received from a status daemon autonomously operating on for the one such network appliance;

obtaining a catalog of currently installable components dynamically generated for the one such network appliance based on the status report independently received from the one such network appliance; and

determining non-current components by comparing the components and versions listed in the obtained catalog against the internal catalog;

wherein each network appliance, prior to sending the status report, executes at least one initial plug-in; and, after installing the installable components, executes at least one post-plug-in;

wherein the at least one initial plug-in monitors the status daemon to determine if the status daemon is running, and restart the status daemon if it is determined that the status daemon is not running;

wherein the catalog further includes a tag indicating a component server at which to locate and obtain each installable component, and a type indicator indicating whether each installable component is a package or a file;

wherein a secure session is negotiated with the one such network appliance utilizing Secure Hypertext Transfer Protocol (HTTPS);

wherein a user identifier associated with the one such network appliance from which the status report is received and a time the status report is received are recorded.

40. (cancelled)

41. (canceled)

42. (canceled)

43. (original): A method according to Claim 39, further comprising:

broadcasting a query message to each such network appliance to trigger a status report.

44. (original): A method according to Claim 39, wherein the components comprise at least one self-installable package, further comprising:

obtaining the at least one self-installable package; and

installing the at least one self-installable package per instructions encoded therein.

45. (original): A method according to Claim 44, wherein the components further comprise at least one file dependent on the at least one self-installable package, further comprising:

obtaining the at least one file subsequent to installing the at least one self-installable package; and

installing the at least one self-installable package per instructions stored in a pre-determined entry.

46. (original): A method according to Claim 44, further comprising:

negotiating a non-secure session prior to obtaining the at least one self-installable package.

47. (original): A method according to Claim 44, further comprising:

at least one of authenticating and decrypting the at least one self-installable package prior to installing the at least one self-installable package.

48. (original): A method according to Claim 44, wherein the instructions comprise an executable installation program plus one or more files to be installed.

49. (original): A method according to Claim 39, wherein the components further comprise at least one file, further comprising:

obtaining the at least one file; and

installing the at least one self-installable package per instructions stored in a pre-determined entry.

50. (currently amended): A method according to Claim 49, further comprising:

negotiating [a]the secure session prior to obtaining the at least one self-installable package.

51. (original): A method according to Claim 49, wherein the pre-determined entry comprise a file information subdirectory identifying installation instructions.

52. (original): A method according to Claim 39, wherein at least one such network appliance performs one of electronic mail anti-virus scanning, content filtering, packet routing, and file, Web and print servicing.

53. (original): A method according to Claim 39, wherein the distributed computing environment is TCP/IP-compliant.

54. (currently amended): A computer-readable storage medium holding code for performing the method according to Claims 39,[40,] 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, or 53.

55. (new): A system according to Claim 1, wherein the status report contains machine-specific data including a load on a processor and available disk space associated with each network appliance, and the application-specific data includes a number of e-mails passing through each of a plurality of network devices.

56. (new): A system according to Claim 1, wherein the installable components for being installed on each network appliance are installed on each network appliance according to a location identified in a corresponding file information subdirectory of the network operations center.